TESTIMONY OF DEIRDRE MULLIGAN

STAFF COUNSEL

OF

THE CENTER FOR DEMOCRACY AND TECHNOLOGY

BEFORE

THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND

TRANSPORTATION

SUBCOMMITTEE ON COMMUNICATIONS

JULY 27, 1999

I. Overview

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify about privacy in the online environment. CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies. We thank the Chairman and Senators Wyden and Hollings for holding this hearing and for their commitment to seeking policies that support both civil liberties and a vibrant Internet.

CDT wishes to emphasize three points this morning:

The Internet presents new challenges and opportunities for the protection of privacy. Our policies must be grounded in an understanding of the medium's unique attributes and its unique potential to promote democratic values.

Privacy is a complex value. In the context of this discussion, we believe Congress should focus on ensuring that individuals' long-held expectations of autonomy, fairness, and confidentiality are respected as daily activities move online. These expectations exist vis-à-vis both the public and the private sectors.

> By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified.

Fairness requires policies that provide individuals with control over information that they provide to the government and the private sector. The concept of fairness is embodied in the Code of Fair Information Practices[1] --long-accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared."[2]

[1] The Code of Fair Information Practices as stated in the Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens,* U.S. Dept. of Health, Education and Welfare, July 1973:

There must be no personal data record-keeping systems whose very existence is secret.

There must be a way for an individual to find out what information about him is in a record and how it is used.

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

There must be a way for the individual to correct or amend a record of identifiable information about him.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. Id. at xx

The Code also requires that those who collect and use personal information do so in a manner that respects individuals' privacy interests. Self-regulatory efforts designed for the online environment are gradually moving closer to the standards for privacy protection set out in the Code of Fair Information Practices. However, legislation, as well as robust self-regulation, is both inevitable and necessary to ensure privacy protection is the rule rather than the exception on the Internet. The Children's Online Privacy Protection Act, which originated in the full Committee, enacted last October provides a model for establishing such a legal framework. The Online Privacy Protection Act of 1999 (S. 809), with modifications, would provide a similar framework for protecting adult privacy and establishing the authority of the Federal Trade Commission to punish back actors.

> In terms of confidentiality, we need a strong Fourth Amendment in cyberspace. But confidentiality protections -- both technical and legal -- are growing increasingly porous as technology changes and more information resides outside of the home on networks. It is time to update and strengthen the Electronic Communications Privacy Act. Further, our laws protecting privacy must be extended to take account of the global nature of the medium. Finally, to ensure that citizens and businesses have the ability to protect their sensitive information and communications, the government must change its policy course on encryption.

Preserving these core elements of privacy on the Internet requires a thoughtful, multi-faceted approach combining self-regulatory, technological, and legislative components.

II. What Makes the Internet Different?

The Code of Fair Information Practices as stated in the *OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data* http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV_EN.HTM

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.

5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him:

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and,
- in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

[2] Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967), 7.

CDT focuses much of its work on the Internet because we believe that it, more than any other medium, has characteristics—architectural, economic, and social—that are uniquely supportive of democratic values. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to "publish" and engage in commerce. Users can reach and create communities of interest despite geographic, social, and political barriers. As the World Wide Web grows to fully support voice, data, and video, it will become in many respects a virtual "face-to-face" social and political milieu.

But while the First Amendment potential of the Internet is clear, and recognized by the Supreme Court, the impact of the Internet on individual privacy is less certain. Will the online environment erode individual privacy—building in national identifiers, tracking devices, and limits on autonomy? Or will it breathe new life into privacy—providing protections for individuals' long held expectations of privacy?

The Internet poses both challenges and opportunities to protecting privacy. The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy. However, Anonymizers, anonymous remailers, and other privacy-enhancing tools allow individuals to create zones of privacy -- limiting who knows what about them and protecting their sensitive communications from prying eyes. Computer code and products are becoming increasingly critical to the protection of privacy in this distributed environment. With privacy-enhancing tools users will be empowered to control their personal information in new ways.

As we move swiftly toward a world of electronic democracy, electronic commerce and indeed electronic living, it is critical to construct a framework of privacy protection that fits with the unique opportunities and risks posed by the Internet. But as Congress has discovered in its attempts to regulate speech, this medium deserves its own analysis. Laws developed to protect interests in other media should not be blindly imported. To create rules that map onto the Internet, we must fully understand the characteristics of the Internet and their implications for privacy protection. We must also have a shared understanding of what we mean by privacy. Finally we must assess how to best use the various tools we have for implementing policy—law, computer code, industry practices, and public education—to achieve the protections we seek.

The Erosion of Privacy and the Path Towards its Restoration

There are several core "privacy expectations" that individuals have long held vis-à-vis both the government and the private sector, the protection of which should carry over to interactions on the Internet. Surveys of Internet users, and would-be Internet users, reveal a high level of concern with threats to privacy online. Surveys suggest that concern over privacy is keeping individuals off the Internet[3], retarding the growth of e-commerce[4], and leading individuals to engage in privacy-protective behaviors such as providing false information.[5] A recent survey of Internet users found that 87% are concerned about threats to their personal privacy.[6]

The remainder of our testimony will discuss the three critical privacy expectations of autonomy, fairness, and confidentiality, explore the changes in technology and policies that threaten them, and finally outline a plan for their restoration.

The Expectation of Autonomy

Why is it at risk?

Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet.

When individuals surf the World Wide Web, they have a general expectation of anonymity, more so than in the physical world where an individual may be observed by others. As documented in several surveys, individuals value their anonymity and will take

[3] A 1998 Business Week Survey found that privacy was the number one reason individuals are choosing to stay off the Internet, coming in well ahead of cost, concerns with complicated technology, and concerns with unsolicited commercial email. Business Week, March 16, 1998.

[4] A TRUSTe and Boston Consulting Group survey conducted in 1997 found that privacy concerns were leading users to limit their engagement in electronic commerce.

[5] Id. and see footnote 6.

[6] *Beyond Concern: Understanding Net Users Attitudes About Online Privacy*, AT&T, 1999.

[7] The *8th annual poll of the Grahpics, Visualization, and Usability Center at the Georgia Institue of Technology* found that in order to protect their privacy, significant numbers of people falsify information online. Particularly, users report regularly falsifying registration information. The most common reason for not registering is the lack of a statement about how the information will be used. In addition, the GVU study showed that users would rather not access a site than reveal information. (1998)

The survey *Beyond Concern: Understanding Net Users Attitudes About Online Privacy* found that individuals were reluctant to provide identifying information such as credit card numbers but were more willing to provide information that did not identify them. AT&T (1999)

steps, such as providing false information and refusing to register, to protect it.[7] Online, individuals often believe that if they have not affirmatively disclosed information about themselves, then no one knows who they are or what they are doing. But, contrary to this belief, the Internet generates an elaborate trail of data detailing every stop a person makes. The individual's employer may capture this data trail if she logs on at work, and it is captured by the Web sites the individual visits. This transactional or click stream data can provide a "profile" of an individual's online life.

Two recent examples highlight the manner in which individuals' expectation of autonomy is increasingly challenged in the online environment. (1) The introduction of the Pentium III processor equipped with a unique identifier (Processor Serial Number) threatens to greatly expand the ability of Web sites to surreptitiously track and monitor online behavior. The PSN could become something akin to the Social Security Number of the online world – a number tied inextricably to the individual and used to validate one's identity throughout a range of interactions with the government and the private sector. (2) The Child Online Protection Act (COPA), passed in October, requires Web sites to prohibit minors' access to material considered "harmful to minors." Today, when an individual walks into a convenience store to purchase an adult magazine, they may be asked to show some identification to prove their age. Under the COPA, an individual will be asked not only to show their identification, but also to leave a record of it and their purchase with the online store. Such systems will create records of individuals' First Amendment activities, thereby conditioning adult access to constitutionally protected speech on a disclosure of identity. This poses a Faustian choice to individuals seeking access to information -- protect privacy and lose access or exercise First Amendment freedoms and forego privacy.

The Path to Individual Autonomy Online

While the global, distributed environment of the Internet raises challenges to our traditional methods of implementing policy, the specifications, standards, and technical protocols that support the operation of the Internet offer a new way to implement policy decisions. In the area of autonomy, focusing on standards and applications is crucial. By building systems that respect individuals varied needs for identification, pseudonymity,

[7] The *8th annual poll of the Grahpics, Visualization, and Usability Center at the Georgia Institue of Technology* found that in order to protect their privacy, significant numbers of people falsify information online. Particularly, users report regularly falsifying registration information. The most common reason for not registering is the lack of a statement about how the information will be used. In addition, the GVU study showed that users would rather not access a site than reveal information. (1998)

The survey *Beyond Concern: Understanding Net Users Attitudes About Online Privacy* found that individuals were reluctant to provide identifying information such as credit card numbers but were more willing to provide information that did not identify them. AT&T (1999)

and anonymity -- building a digital wallet with cash, credit cards, a metro fare card, and a driver's license -- will help build an online environment that promotes autonomy. By building privacy into the architecture of the Internet, we have the opportunity to advance public policies in a manner that scales with the global and decentralized character of the network. As Larry Lessig repeatedly reminds us, "(computer) code is law."

Accordingly, we must promote specifications, standards and products that protect privacy. A privacy-enhancing architecture must incorporate, in its design and function, individuals' expectations of privacy. For example, a privacy-friendly architecture would provide individuals the ability to "walk" through the digital world, browse, and even purchase without disclosing information about their identity, thereby preserving their autonomy. Of course, it would also provide individuals the opportunity to create relationships that are identifiable -- or at least authenticated -- for engaging in activities such as banking. This would be coupled with policies that allow individuals to control when, how, and to whom personal data collected during interactions is used or disclosed.

While there is much work to be done in designing a privacy-enhancing architecture, some substantial steps toward privacy protection have occurred. Positive steps to leverage the power of technology to protect privacy can be witnessed in tools like the Anonymizer, Crowds, and Onion Routing, which shield individuals' identity during online interactions, and encryption tools such as Pretty Good Privacy that allow individuals to protect their private communications during transit. Coupled with rules such as those found in the Government Paperwork Elimination Act of 1998, which established privacy protections governing personal information collected when the public uses electronic signature systems,[8] technology may evolve in ways that support individuals' interest in autonomy.

The Expectation of Fairness and Control Over Personal Information

Who controls the data?

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will collect only information necessary to perform the service and use it only for that purpose. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, current practices, both offline and online, foil this expectation of privacy. Much of the concern with privacy in electronic commerce stems from a lack of privacy rules in various sectors of the economy, such as

[8] .Many such systems gather sensitive information in the course of providing and guaranteeing an electronic signature.

The law prohibits companies that collect such information from using or disclosing it without the permission of the person involved. Authored by Senators Leahy and Abraham, this marks the first attempt to craft a legislative approach to dealing with the potential erosion of privacy created by electronic signature use.

financial and health, that handle a treasure trove of sensitive information on individuals. Whether it is medical information, or a record of a book purchased at the bookstore, or information left behind during a Web site visit, information is routinely collected without the individual's knowledge and used for a variety of other purposes without the individual's knowledge—let alone consent.

Focusing on the online environment, we now have information from two studies assessing the state of privacy notices on the World Wide Web. Last June, the Federal Trade Commission's "Privacy Online: A Report to Congress" found that despite increased pressure, businesses operating online continued to collect personal information without providing even a minimum of consumer protection. The report looked only at whether Web sites provided users with notice about how their data was to be used; there was no discussion of whether the stated privacy policies provided adequate protection. The survey found that, while 92% of the sites surveyed were collecting personally identifiable information, only 14% had some kind of disclosure of what they were doing with personal data.

The newly released Georgetown Internet Privacy Policy Survey provides new data. The Survey was designed to provide an update on the state of privacy policies on the World Wide Web. The study shows that definite progress has been made in making many more Web sites privacy-sensitive, but substantive privacy protections are still far from ubiquitous on the World Wide Web. While more Web sites are mentioning privacy, *only 9.5%* provide the types of notices *required* by the Online Privacy Alliance, the Better Business Bureau and TRUSTe. Indeed, fair information practices on the Web appear to remain the exception, not the rule.

The Georgetown Survey shows that, spurred by surveys documenting consumer concern and anxiety, and the work of individual companies[9] and industry self-regulatory entities such as TrustE, the Online Privacy Alliance, and the Better Business Bureau, an increased number of Web sites are providing consumers with *some* information about what personal information is collected (44%), and how that information will be used (52%). Companies posting fuller information about their data handling[10] are more likely to make them accessible to consumers. Many have a link to such statements from the home page (79.7%).[11]

[9] For example, IBM recently stated that it would limit its advertising to Web sites that post privacy notices.

[10] The report calls these "privacy policies" as compared to "information practice statements." "Privacy policies" are a more comprehensive description of a site's practices that are located in a single place and accessible through an icon or hyperlink. A site may have a "privacy policy" by this definition but still not have a privacy policy that meets the elements set out by the FTC or various industry self-regulatory initiatives for an adequate privacy policy.

[11] In response to the question, "Is a Privacy Policy Notice easy to find?" surfers in the 1998 survey answered yes for approximately 1.2% of Web sites. FTC Report, Appendix C Q19.

However, on important issues such as access to personal information and the ability to correct inaccurate information, the Georgetown Survey shows that only 22% and 18% respectively of these highly trafficked Web sites provide consumers with notice. On the important issue of providing individuals with the capacity to control the use and disclosure of personal information, the survey finds that 39.5% of these busy Web sites say that consumers can make some decision about whether they are re-contacted for marketing purposes -- most likely an "opt-out" -- and fewer still, 25%, say they provide consumers with some control over the disclosure of data to third parties.[12]

Overall, the Georgetown survey reveals that, at over 90% of the most frequently trafficked Web sites,[13] consumers are not being adequately informed about how their personal information is handled.[14] At the same time the survey found that over 90% of these same busy consumer-oriented Web sites are collecting personal information.[15] In fact, the survey revealed an increase in the number of Web sites collecting sensitive information such as credit card numbers (up 20%), names (up 13.3%), and even Social Security Numbers (up 1.7%).

Thus, while many companies appear to be making an effort to address some privacy concerns, the results from the consumer perspective appear to be a quilt of complex and inconsistent statements. The number of sites that provide consumers with the types of notices required by the Online Privacy Alliance, the Better Business Bureau and TrustE, and called for by the Federal Trade Commission and the Administration, is still relatively small (9.5%).

The posting of privacy notices is not just a private sector issue. In a recent CDT study of federal agency Web sites, we found that just over one-third of federal agencies had a "privacy notice" link from the agency's home page. Eight other sites had privacy policies that could be found after following a link or two and on 22 of the sites surveyed we could not find a privacy policy at all.

The lack of widespread adherence to Fair Information Practices is undermining consumer confidence. A recent survey by the National Consumers League found that the majority of online users are not comfortable providing credit card (73%), financial (73%), or personal information (70%) to businesses online.[16] Due to privacy concerns 42% of those who use the Internet are using it solely to gather information, while a smaller 24%

[12] This number is generated using the data from Q32 (number of sites that say they give consumers choice about having collected information disclosed to outside third parties) -- 64 -- and dividing it by 256 (the total survey sample (364) minus the number of sites that affirmatively state they do not disclose data to third-parties (Q29A) (69) and the number of sites that affirmatively state that data is only disclosed in the aggregate (Q30) (39)).

[13] Only 9.5% of the most frequently visited Web sites and 14.7% of those that collect information had privacy policies containing critical information called for by the FTC, the Administration, and required by the Online Privacy Alliance, TrutstE and the BBB Online, about notice; choice; access; security; and contact information.

[14] Last years survey found approximately 2% or Web sites that collected data, and less than 1% of all Web sites, had adequate notices.

[15] 92.9% are collecting some type of personal information.

[16] *Consumers and the 21st Century*, National Consumers League (1999).

[17] Id.

actually venture to purchase goods online.[17] A second study found that 58% of consumers do not consider financial transactions online to be safe, and 77% do not believe it is safe to provide a credit card number through a computer.[18] Privacy has been rightly identified by the Federal Trade Commission, Congress, the business community, and advocacy organizations as a critical consumer protection issue in e-commerce.

Establish Rules That Give Individuals Control Over Personal Information During Commercial Interactions

We must adopt enforceable standards, both self-regulatory and legislative, to ensure that information provided for one purpose is not used or redisclosed for other purposes without the individual's consent. All such efforts should focus on the Code of Fair Information Practices developed by the Department of Health, Education and Welfare in 1973. The challenge of implementing privacy practices on the Internet is ensuring that they build upon the medium's real-time and interactive nature to foster privacy and that they do not unintentionally impede other beneficial aspects of the medium. Implementing privacy protections on the global and decentralized Internet is a complex task that will require new thinking and innovative approaches.

The Georgetown Survey supports our belief that a combination of means – self-regulation, technology, and legislation – are required to provide privacy protections on the Internet. The study, as discussed above, shows that some progress has been made in making many more Web sites privacy sensitive, but substantive privacy protections are still far from ubiquitous on the World Wide Web. Because many Web sites need baseline policy guidance and because self-enforcement mechanisms, while emerging, may not always provide a viable remedy, we believe that legislation is both inevitable and necessary to ensure consumers' privacy on the Internet.

To achieve real privacy on the Internet, we will need more than better numbers, redoubled efforts by industry, or a legislative mantra. We will need a good-faith concerted effort by industry, consumer and privacy advocates, and policymakers to develop real and substantive answers to a number of difficult policy issues involving the scope of identifiable information, the workings of consent and access mechanisms, and the structure of effective remedies that protect privacy without adversely affecting the openness and vitality of the Internet.

As the Federal Trade Commission's rulemaking under the Children's Online Privacy Protection Act and industry's various efforts at self-regulation show, these issues are not easy. But armed with the findings of the Georgetown

[17] Id.
[18] *National Technology Readiness Survey*, conducted by Rockridge Associates (1999).

Internet Privacy Policy Survey, we believe interested parties are in a position to move forward on a three pronged approach – expanded self-regulation, work to develop and deploy privacy-enhancing technologies such as P3P, and legislation – all require a serious dialogue on policy and practice options for resolving difficult issues in this promising medium.

In its testimony last July, the Federal Trade Commission stated that, "…unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional governmental authority in this area would be appropriate and necessary."[19] Despite the considerable effort of Congress, the Federal Trade Commission, the Administration and industry to encourage and facilitate an effective self-regulatory system to protect consumer privacy, based on the survey results we do not believe that one has yet emerged. Like Commissioner Anthony, we believe that industry leadership and self-regulatory programs are a critical component of a privacy framework for the Internet, but that legislation is also necessary to establish a baseline and ensure consumers are protected from bad actors.

Last year, the Federal Trade Commission offered a legislative outline that embodied a framework, similar to the one we suggest, building upon the strengths of both the self-regulatory and regulatory processes. This year several bills have been introduced on a wide range of privacy issues.[20] The Online Privacy Protection Act[21] introduced by Senators Burns and Wyden is substantially similar to the model recommended by the Federal Trade Commission last year. (Specific comments on the Online Privacy Protection Act can be found in subsection 3 below.)

Historically, for privacy legislation to be successful, it must garner the support of at least a section of the industry. To do so, it generally must build upon the work of some industry members—typically binding bad actors to the rules being followed by industry leaders—or be critically tied to the viability of a business service or product as with the Video Privacy Protection Act and the Electronic Communications Privacy Act. Several

[19] Last years survey found approximately 2% or Web sites that collected data, and less than 1% of all Web sites, had adequate notices. Privacy Online: A Report to Congress, Federal Trade Commission, June 1998.

[20] Electronic Rights for the Twenty-First Century Act of 1999 (E-RIGHTS) (S. 854), introduced on April 21, 1999 by Senator Leahy (D-VT). The Online Privacy Protection Act of 1999 (S. 809), introduced on April 15, 1999, by Senators Burns (R-MT) and Wyden (D-OR). Internet Growth and Development Act of 1999 (H.R. 1685), introduced on May 5, 1999 by Representatives Boucher (D-VA) and Goodlatte (R-VA). Consumer Internet Privacy Protection Act of 1999 (H.R. 313), introduced on January 6, 1999, by Representative Vento (DFL-MN). We anticipate additional proposals from Senators Kohl, Torricelli, Dewine, and Hatch, and Representative Markey

[21] The Online Privacy Protection Act of 1999 (S. 809), introduced on April 15, 1999, by Senators Burns (R-MT) and Wyden (D-OR).

companies have staked out leadership positions on the issue of online privacy and several self-regulatory programs have formed to drive industry best practices online. Numerous surveys have documented that consumers are concerned about their privacy in e-commerce.

In addition to work on policies, there is important activity in the technical community on how to develop the tools necessary to implement fair information practices on the World Wide Web. The World Wide Web Consortium's Platform for Privacy Preferences ("P3P") is a promising development. The P3P specification will allow individuals to query Web sites for their policies on handling personal information and to allow Web sites to easily respond. While P3P does not drive the specific practices, it is a standard designed to promote openness about information practices, to encourage Web sites to post privacy policies and to provide individuals with a simple, automated method to make informed decisions. Through settings on their Web browsers, or through other software programs, users will be able to exercise greater control over the use of their personal information. Regardless of how policies are established, an Internet-centric method of communicating about privacy is part of the solution.

As Congress moves forward this year, we look forward to working with you and all interested parties to ensure that fair information practices are incorporated into business practices on the World Wide Web. Both legislation and self-regulation are only as good as the substantive policies they embody. As we said at the start, crafting meaningful privacy protections that map onto the Internet requires us to resolve several critical issues. While consensus exists around at least four general principles (a subset of the Code of Fair Information Practices) – notice of data practices; individual control over the secondary use of data; access to personal information; and, security for data – the specifics of their implementation and the remedies for their violation must be explored. We must wrestle with difficult questions: When is information identifiable? How is it accessed? How do we create meaningful and proportionate remedies that address the disclosure of sensitive medical information as well as the disclosure of inaccurate marketing data? For the policy process to successfully move forward these hard issues must be more fully resolved. We would welcome the opportunity to work with Senators Burns and Wyden, and other members of this committee, to explore these issues and develop a framework for privacy protection in the online environment. The Online Privacy Protection Act could serve as a starting point for this discussion. The leadership of Internet-savvy members of this Committee and others will be critical as we seek to provide workable and effective privacy protections for the Internet.

3. Preliminary Comments on the Online Privacy Protection Act (S. 809) and suggested changes

The Online Privacy Protection Act is closely modeled on the Children's Online Privacy Protection Act enacted last year. It establishes baseline practices for commercial Web sites handling personal information and provides the Federal Trade Commission with authority to enforce violations of the Act.

Legislation to protect privacy should be based on the Code of Fair Information Practices which has served as a model for privacy legislation and self-regulatory codes in the United States and across the globe for twenty-five years.

The Code of Fair Information Practices requires that businesses collecting personal information (record keepers):

Be publicly identified and provide a description of the purpose and uses they make of personal information.

Limit the personal information they collect to what is necessary to support the purpose of collection. Personal information must be collected by lawful and fair means and, where appropriate, with the knowledge and consent of the individual.

Limit the use and disclosure of personal information to the purpose for which it was collected, unless the individual has granted consent.

Ensure that personal information collected is relevant to the purpose of collection, accurate, timely, and complete.

Institute reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification and disclosure.

Be accountable for complying with fair information practices.

The Code of Fair Information Practices says that individuals should have the right to:

Access personal information and to correct or remove data that is not timely, accurate, relevant, or complete; and, to

Control the use of personal information. Personal information provided to a business may not be used or disclosed for other purposes without the consent of the individual or other legal authority.

To bring the Online Privacy Protection Act (S. 809) in line with the Code of Fair Information Practices we recommend the following changes.

Section 2(b)(1)
Individual Control

To ensure that individuals are able to control the use of their personal information, Section 2(b)(1) (A)(ii) should require Web sites to gain individuals

consent to the use and disclosure of personal information for purposes unrelated to the purpose for which it was obtained. The range of personal information that will be exchanged on Web sites runs from the highly sensitive -- financial and health -- to contact information such as email and address. Surveys indicate that individuals desire control over their personal information: consent is the surest method of providing consumers with this control. On the Internet we believe that the distinction between "opt-out" and "opt-in" may become less important as technology enables individuals to exercise control over how, when, for what purposes, and under what conditions they disclose personal information.

The bill summary suggests that the intent of the proposal is to provide individuals with the ability to "opt-out" of having their information used and disclosed. However, as currently drafted this section does not require Web sites to gain the individual's consent, nor does it provide an " opt-out" for the collection or use of information -- it requires an "opt-out" be provided where information will be disclosed to others. In addition, section 2) of this provision could be read to allow Web sites to forego offering individuals even an opt-out if in the notice they tell individuals that they disclose information.

Access and Correction

To ensure that individuals are able to review and correct personal information about themselves, section (B)(i) should be amended to require Web sites to provide individuals with access to all personal information regardless of whether it is used internally, or sold or transferred to other companies.

Section 2(b)(2)
Limits on Disclosure

We have questions about the purpose of this section. However, at this time, we recommend eliminating subsections (A) and (B) and amending (C) by changing the word "permitted" to "required." Thus the provision would allow a Web site to disclose personal information where "required under other provisions of law."

Section 2(b)(3)
Limits on Access

We have questions about the purpose of this section. However, at this time, we recommend eliminating subsections (A), (B) and (E). Section (C) should be rewritten to limit access to information that is trade secret.

Additional comments

The scope of the bill is information collected online – this means that information collected by Web sites from other sources is not governed by the bill. It is unclear whether consumers, and businesses, distinguish between interactions conducted online and offline with the same entity. As the Committee moves forward, it should consider whether the online/offline distinction is meaningful to consumers and the business community.

Several issues have surfaced during the Federal Trade Commission's Rulemaking under the Children's Online Privacy Protection Act that would benefit from additional consideration by this Committee. They include: what does it mean to "collect" information in the online context; when is information personally identifiable; and, what does it mean to "contact" an individual online. In addition, the Children's Online Privacy Protection Act, and the proposed Online Privacy Protection Act, give enforcement authority to the Federal Trade Commission while other privacy statutes tend to provide individuals with private rights of actions to address grievances. Arguments can be made in favor and against each model of oversight and enforcement: exploring the effectiveness of each (or a combination thereof) would be useful in crafting meaningful remedies for individuals and successful oversight mechanisms.

C. The Expectation of Confidentiality

1. Who has access to records in cyberspace?

When individuals send email they expect that only the intended recipient will read it. In passing the Electronic Communications Privacy Act in 1986, Congress reaffirmed this expectation. Unfortunately, it is once again in danger.

While United States law provides email the same legal protection as a first class letter, the technology leaves unencrypted email as vulnerable as a postcard. Compared to a letter, an email message is handled by many independent entities and travels in a relatively unpredictable and unregulated environment. To further complicate matters, the email message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the privacy protections are likely to stop at the border.

Email is just one example. Today our diaries, medical records, and confidential documents are more likely to be out in the network than stored in our homes. As our wallets become “e-wallets” housed somewhere out on the Internet rather than in our back-pockets, the confidentiality of our personal information is at risk. The advent of online datebooks, and products such as Novell’s “Digital

Me", and sites such as Wellmed.com[22] which invite individuals to take advantage of the convenience of the Internet to manage their lives, financial information, and even medical records raise increasingly complex privacy questions. While the real "me" has Fourth and Fifth Amendment protections from the government, the "Digital Me" is increasingly naked in cyberspace.

2. Protecting the Privacy of Communications and Information

Increasingly, our most important records are not "papers" in our "houses" but "bytes" stored electronically at distant "virtual" locations for indefinite periods of time and held by third parties. The Internet, and digital technology generally, accelerate the collection of information about individuals' actions and communications. Our communications, rather than disappearing, are captured and stored on servers controlled by third parties. Daily interactions such as our choice of articles at a news Web site, our search and purchase of an airline ticket, and our use of an online date book, such as Yahoo's calendar, leave detailed information in the hands of third-parties. With the rise of networking and the reduction of physical boundaries for privacy, we must ensure that privacy protections apply regardless of where information is stored.

Under our existing law, there are now essentially four legal regimes for access to electronic data: 1) the traditional Fourth Amendment standard for records stored on an individual's hard drive or floppy disks; 2) the Title III-Electronic Communications Privacy Act standard for records in transmission; 3) the standard for business records held by third parties, available on a mere subpoena to the third party with no notice to the individual subject of the record; and 4) a statutory standard allowing subpoena access and delayed notice for records stored on a remote server, such as the diary of a student stored on a university server, or personal correspondence stored on a corporate server.

As the third and fourth categories of records expand because the wealth of transactional data collected in the private sector grows and people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment.

[22] WellMed.com is a proprietary Online Health Management System which works by collecting personal health information from individuals, analyzing that information to develop unique health profiles which are used for a variety of purposes. One service is HealthNow! -- "an online personal health record enabling secure, confidential, and private storage, management, and maintenance of health information by individuals and their families. HealthNow affords easy access of medical records from one central location anytime and anywhere the need arises."

Congress took the first small step towards recognizing the changing nature of transactional data with amendments to the Electronic Communications Privacy Act enacted as part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). But the ongoing and accelerating increase in transactional data and the detail it reveals about individuals' lives suggests that these changes are insufficient to protect privacy.

Moreover, the Electronic Communications Privacy Act must be updated to provide a consistent level of protection to communications and information regardless of where they are stored and how long they have been kept. Senator Leahy's recently introduced legislation is an effort to restore 4th Amendment protections to our personal papers. Technologies that invite us to live online will quickly create a pool of personal data with the capacity to reveal an individual's travels, thoughts, purchases, associations, and communications. We must raise the legal protections afforded to this growing body of detailed data regardless of where it resides on the network.

Conclusion

No doubt, privacy on the Internet is in a fragile state. Providing protections for individual privacy is essential for a flourishing and vibrant online community and marketplace. It is clear that our policy framework did not envision the Internet as we know it today, nor did it foresee the pervasive role information technology would play in our daily lives. Our legal framework for protecting individual privacy in electronic communications, while built upon constitutional principles buttressed by statutory protections, reflects the technical and social "givens" of specific moments in history. Crafting privacy protections in the electronic realm has always been a complex endeavor. Reestablishing protections for individuals' privacy in this new environment requires us to focus on both the technical aspects of the Internet and on the practices and policies of those who operate in the online environment.

However, there is new hope for the restoration of privacy. Providing a web of privacy protection to data and communications as they flow along networks requires a unique combination of tools—legal, policy, technical, and self-regulatory. We believe that legislation is an essential element of the online privacy framework and we look forward to working with this committee on the Online Privacy Protection Act (S. 809) and other proposals. Whether it is setting limits on government access to personal information, ensuring that a new technology protects privacy, or developing legislation all require discussion, debate, and deliberation. We thank the Committee for the opportunity to share our views and look forward to working with the members

and staff and other interested parties to foster privacy protections for the Digital Age.